

Amendments To The Claims

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for computer network access comprising the steps of:
running a client application wherein,
the client application is not a web browser, and
the client application runs on a customer device;
entering user information into the customer device;
communicating the entered user information to a first server;
storing the user information on the first server;
creating a unique customer identification for a user of the customer device;
storing the unique customer identification on the first server;
communicating the unique customer identification to,
a client running the client application, and
other servers running a plurality of server applications;
wherein the communication does not include a cookie sent to a browser[.];
storing the unique customer identification
on the client and
the other servers;
communicating the unique customer identification from the client to the first server or
one of the other servers; and
authenticating the user by matching the unique customer identification received at the
first server or one of the other servers with the unique customer identification stored on the first
server or one of the other servers.
2. (Currently Amended) The method of claim 1 wherein
in the step of authenticating the user by matching the unique customer identification, the
first server and each of the other servers has a particular service available to the user of the

customer device and

the user of the customer device is not allowed access to the particular service if the unique customer identification received at the server does not match the stored unique customer identification.

3. (Previously Presented) The method of claim 1 wherein in the step of communicating the entered user information to a first server the communication is compliant with a common gateway interface standard.

4. (Previously Presented) The method of claim 1 wherein in the step of communicating the entered user information a JAVA servlet technology is used.

5. (Previously Presented) The method of claim 1 wherein in the step of communicating the entered user information a Berkeley System Distribution socket interface is used.

6. (Previously Presented) The method of claim 1 wherein in the step of communicating the unique customer identification the communication complies with a common gateway interface standard.

7. (Previously Presented) The method of claim 1 wherein in the step of communicating the unique customer identification a JAVA servlet technology is used.

8. (Previously Presented) The method of claim 1 wherein in the step of communicating the unique identification a Berkeley System Distribution socket interface is used.

9. (Previously Presented) A digital computer system programmed to perform the following steps:

run a client application wherein,

the client application is not a web browser, and

the client application runs on a customer device;
receive user information entered into the customer device;
communicate the entered user information to a first server;
store the user information on the first server;
create a unique customer identification for a user of the customer device;
store the unique customer identification on the first server;
communicate the unique customer identification to,
a client running the client application, and
other servers running a plurality of server applications
wherein the communication does not include a cookie sent to a browser;
store the unique customer identification on the client and the other servers;
communicate the unique customer identification from the client to the first server or one
of the other servers; and
authenticate, the user by matching the unique customer identification received at the first
server or one of the other servers with the unique customer identification stored on the first
server or one of the other servers
wherein each of the other servers has a particular service available to the user of the
customer device and
wherein the user of the customer device is not allowed access to the services the unique
customer identification received at the first server or one of the other servers does not match the
unique customer identification stored on the first server or one of the other servers.

10. (Currently Amended) A computer-readable medium storing a computer program, the
computer program functional to perform the following steps:

run a client application wherein,
the client application is not a web browser, and
the client application runs on a customer device;
receive user information entered into the customer device;
communicate the entered user information to a first server;

store the user information on the first server;
create a unique customer identification for a user of the customer device;
store the unique customer identification on the first server;
communicate the unique customer identification to,
 a client running the client application, and
 other servers running a plurality of server applications;
store the unique customer identification on the client and the other servers;
communicate the unique customer identification from the client to the first server or one
of the other servers; and
 authenticate, the user by matching the unique customer identification received at the first
server or one of the other servers with the unique customer identification stored on the first
server or one of the other servers[.];
 wherein each of the other servers has a particular service available to the user of the
customer device and
 wherein the user of the customer device is not allowed access to the services the unique
customer identification received at the first server or one of the other servers does not match the
unique customer identification stored on the first server or one of the other servers.

11. (Currently Amended) A computer network system comprising:

 a server computer running a server software application operable to;
 create a unique customer identification for a user,
 store the unique identification on the server computer,
 communicate the unique customer identification to a client, wherein the
communication does not include a cookie sent to a browser; and
 authenticate the user via the unique identification when the user communicates
with the server computer; and
 a client computer running a client software application said client computer operably
connected to the server computer over a network and wherein the client software application is
operable to:

communicate user information to the server application,
store the unique customer ~~identification~~ identification, and
provide the server with the unique customer ~~identification~~ identification to
authenticate a user with the server application; and

at least one additional server computer running an additional server software application,
said additional server computer operably connected to the server computer and client computer
over a network and operable to provide information services to the user, and operable to receive
the unique customer identification from the server computer and authenticate the user via the
unique customer identification when the user communicates with the additional server software
application.

12. (Previously Presented) The computer network system of claim 11 further comprising:

at least one additional server software application running on the server computer
operable to provide information services to the user and operable to receive the unique customer
identification from the server computer and authenticate the user via the unique customer
identification when the user communicates with the additional server software application.

13. (Cancelled) ~~The computer network system of claim 11 further comprising:~~

~~at least one additional server computer running an additional server software application,~~
~~said additional server computer operably connected to the server computer and client computer~~
~~over a network and operable to provide information services to the user, and operable to receive~~
~~the unique customer identification from the server computer and authenticate the user via the~~
~~unique customer identification when the user communicates with the additional server software~~
~~application.~~

14. (Currently Amended) The method of claim 1 wherein the step of creating a unique customer
identification for the user of the consumer device the step ~~includes~~ includes generating a random
number.

15. (Previously Presented) The method of claim 1 wherein in the step of communicating the unique customer identification to the client and other servers the unique identification is not embedded in a cookie.
16. (Previously Presented) The method of claim 1 wherein in the step of communicating the unique customer identification to the client and other servers the unique customer identification is not a cookie.
17. (Previously Presented) The method of claim 1 wherein in the step of communicating user information to a first server from a client the user information includes an address and a phone number.
18. (Previously presented) The computer network system of claim 11 wherein the client software application does not store cookies.
19. (Currently Amended) The computer network of claim ~~[[13]]~~ 11 wherein the at least one additional server computer running is operably connected to the server computer through a business network.
20. (Previously presented) The computer network of claim 19 further comprising a firewall between the one server computer and the client computer.